



**RECEIVED**  
AUG 17 2004  
**GROUP 3600**

## **APPENDIX A**

### **SUBSTITUTE SPECIFICATION FOR**

Method and Apparatus for Providing Postage Indicia Over a Data  
Communication Network

**U.S. Application No. 09/708,913**

**filed November 7, 2000**

# **Method and Apparatus for Providing Postage Indicia Over a Data Communication Network**

## **COPYRIGHT NOTICE**

5           A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the xerographic reproduction by anyone of the patent document or the patent disclosure in exactly the form it appears in the U.S. Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

## **CROSS-REFERENCE TO RELATED APPLICATIONS**

10           The disclosure of the following U.S. Patent Application is herein incorporated by reference in its entirety for all purposes:

          (1) U.S. Non-Provisional Patent Application No. 09/358,801, entitled  
15   “Method And Apparatus For Postage Label Authentication,” filed July 21, 1999.

          The following patent applications, including the present application, are being filed concurrently, and the disclosure of each other application is herein incorporated by reference in its entirety for all purposes:

20           (1) U.S. Non-Provisional Patent Application No. 09/708,883, entitled “Techniques For Dispensing Postage Using A Communication Network”, filed February 9, 2000;

          (2) U.S. Non-Provisional Patent Application No. 09/708,975, entitled  
25   “Method Of Distributing Postage Label Sheets With Security Features”, filed November 7, 2000;

          ([4])3 U.S. Non-Provisional Patent Application No. 09/708,698, entitled “System And Method For Managing Multiple Postage Functions In A Single Account”, filed November 7, 2000;

30           (4) U.S. Non-Provisional Patent Application No. 09/708,792, entitled “Targeted Advertisement Using A Security Feature On A Postage Medium”, filed November 7, 2000;

          (5) U.S. Non-Provisional Patent Application No. 09/708,185, entitled “System And Method Of Printing Labels”, filed November 7, 2000;

(6) U.S. Non-Provisional Patent Application No. 09/708971, entitled "Providing Stamps On Secure Paper Using A Communications Network", filed November 7, 2000;

5 (7) U.S. Non-Provisional Patent Application No. 09/611,375, entitled "Providing Stamps On Secure Paper Using A Communications Network," filed July 7, 2000;

(8) U.S. Provisional Patent Application No. 60/216,779, entitled "System And Method Of Printing Labels," filed July 7, 2000;

10 (9) U.S. Provisional Patent Application No. 60/216,653, entitled "Method And System For Dispensing Postage Over The Internet, With Enhanced Postal Security Features" filed July 7, 2000;

(10) U.S. Provisional Patent Application No. 60/206,207, entitled "Providing Stamps on Secure Paper Using A Communications Network" filed May 22, 2000;

15 (11) U.S. Provisional Patent Application No. 60/204,357, entitled "Stamps Over a Communications Network" filed May 15, 2000;

(12) U.S. Provisional Patent Application No. 60/181,299, entitled "System and Method For Stamps Over The Internet," filed February 9, 2000; and

20 (13) U.S. Provisional Patent Application No. 60/181,368, entitled "System and Method For Stamps Over The Internet," filed February 8, 2000.

## BACKGROUND OF THE INVENTION

The present invention generally relates to dispensing postage, and in particular to computer-based dispensing of postage over a data communication network.

25 Millions of small businesses employ a variety of tools in their daily operations, such as telephones, copying machines, telefax machines, and personal computers (PC's). Of note is the rapid acceptance of PC's in the small business environment. In the past, computers were available only to large companies which could afford the bulky and quite expensive machines. The development and continuing  
30 evolution of semiconductor technology has changed the computer usage model, and has made powerful computing capability available to the general public.

A key component of a business is the mailing and receiving of correspondence, between businesses and with its customers. Consequently, the mechanical postage meter has become a ubiquitous item in most business operations.

However, unlike the proliferation of PC's, conventional postage meters have not achieved the market penetration that other conventional pieces of office equipment have. The primary reason is a perceived high (and recurring) cost of postage meters, which outweighs their convenience in the eyes of potential users.

At the other end of a business operation is the consumer. In the case of the Internet, consumers who purchase goods over the Internet are sometimes faced with the inconvenience of having to return the product. One aspect of that inconvenience is that the consumer does not have access to high denomination stamps that goods may require, or the weighing scale needed to weigh the goods. Consequently, a lengthy and usually tedious trip to the post office is required. This experience is totally at odds with the ease and speed associated with an Internet purchase.

The United States Postal Service (USPS) has promulgated specifications for its Information Based Indicia Program (IBIP). The IBIP program supports new methods of applying postage in lieu of conventional approaches that typically rely on the use of a postage meter mechanically printing the indicium on mailpieces.

The IBIP program contemplates postal indicia printed by conventional printers (e.g., thermal, inkjet, or laser) and including human-readable and machine-readable portions. An indicium refers to the imprinted designation or a postage mark used on mailpieces denoting evidence of postage payment. The machine-readable portion was initially specified to be a two-dimensional barcode symbology known as PDF417. The indicium content includes a digital signature for security reasons (to preclude forgery). There are separate specifications for open and closed systems.

The specifications have been updated over the last few years; the recent specifications for open and closes systems are:

- Information-Based Indicia Program (IBIP) Performance Criteria for Information-Based Indicia and Security Architecture for Open IBI Postage Evidencing Systems (PCIBI-O) (Draft February 23, 2000), and
- Information-Based Indicia Program (IBIP) Performance Criteria for Information-Based Indicia and Security Architecture for Closed IBI Postage Metering Systems (PCIBI-C) (Draft January 12, 1999).

These specifications are incorporated by reference in their entirety for all purposes.

An open system is defined as a general purpose computer used for printing information-based indicia, but not dedicated to the printing of those indicia. A closed

system is defined as a system whose basic components are dedicated to the production of information-based indicia and related functions, that is, a device dedicated to creating indicia similar to an existing, traditional postage meter. A closed system may be a proprietary device used alone or in conjunction with other closely related, specialized equipment, and includes the indicium print mechanism.

The IBIP program specifies a postal security device (PSD) that manages the secure postage registers and performs the cryptographic operations of creating and verifying digital signatures.

The open system specification describes a host system (a computer or postage meter) connected to an unsecured printer (e.g., a laser printer or the like) and a PSD. The host system also provides communication facilities that allow the PSD's vendor and/or the USPS to establish communications with the PSD. Communications supported include troubleshooting, accounting transactions, and the like.

The PSD and host cooperate to provide an indicium, which is then transmitted to and printed by the unsecured printer. The specified indicium allows the use of an unsecured printer (e.g., thermal, inkjet, or laser) by using a digital signature, which also supports authentication of the mail piece. The indicium includes human-readable information and machine-readable information (initially specified as a PDF417 two-dimensional bar code). Each PSD is a unique security device, having core security functions such as digital signature generation and verification and secure management of information (e.g., descending and ascending registers).

U.S. Patent No. 6,005,945 to Whitehouse discloses a system for electronic distribution of postage using a secure central computer which generates postal indicia in response to postage requests submitted by end user computers. However, these conventional techniques, including the system described in the Whitehouse patent, still require the user to apply for and obtain a license. As a result, a user still has to suffer the inconveniences and bureaucratic hurdles of obtaining the license. Thus, even though the conventional electronic postage distribution techniques have reduced the inconveniences associated with traditional postage meters, they are still significantly unwieldy.

A need therefore exists to simplify the attainment of postage using a computer. It is further desirable to provide a computer-based approach that facilitates access to postage by the consuming public.

## SUMMARY OF THE INVENTION

A method and system for obtaining postage in accordance with the invention includes a first server system for receiving requests for postage from users. The first server is in communication with a second server system which dispenses postage to the first server. User-requests for postage received by the first server system are communicated to the second server system. In response, the second server system dispenses postage to the first server system, which then distributes the postage to the user to satisfy the requests for postage.

In one embodiment of the invention, transmission of postage from the second server system in response to a user's request for postage includes verifying for available funds based on a payment mechanism provided by a user to determine whether the requested postage will be dispensed to that user. In another embodiment of the invention, postage is dispensed by the second server system on the basis of a payment mechanism provided by the first server system.

Postage is dispensed by the second server system by transmitting to the first server system information for printing a postage indicium. In an embodiment of the invention, the first server system enhances the information with one or more background images.

## BRIEF DESCRIPTION OF THE DRAWINGS

The teachings of the present invention can be readily understood by considering the following detailed description in conjunction with the accompanying drawings:

Fig. 1 illustrates a typical system arrangement for dispensing postage in accordance with an embodiment of the present invention;

Fig. 2 shows the data transfers that take place during the dispensing of postage in accordance with the illustrative embodiment of the invention shown in Fig. 1;

Fig. 3 shows the processing that takes place during the dispensing of postage in accordance with the illustrative embodiment of the invention shown in Fig. 1;

Fig. 4 depicts an exemplary individual pre-printed label on which an indicium may be printed according to an embodiment of the present invention;

Fig. 5 depicts a sheet of pre-printed labels according to an embodiment of the present invention;

Fig. 6 depicts an individual label with an indicium printed on it according to an embodiment of the present invention;

Fig. 7 is an expanded block diagram of a postage vendor system according to an embodiment of the present invention; and

5 Fig. 8 is a simplified flowchart showing processing performed by the various components of a postage vendor system upon receiving a request to purchase postage according to an embodiment of the present invention.

#### DESCRIPTION OF THE SPECIFIC EMBODIMENTS

10 Fig. 1 shows a data communication system 100 in an illustrative example representative of a typical embodiment of the invention. The system comprises a first data server 102 and a second data server 104. The servers are in data communication over a communications network 122. One or more user systems 132, 134 access first data server 102 via the communication network.

15 Each user (client) 132, 134 typically comprises a conventional personal computing machine (PC) running conventional user software (not shown). Typical PC's include MACINTOSH® PC's from Apple Computer, Inc., INTEL®-compatible PC's, and so on. Data servers 102 and 104 are typically high-end computing machines capable of high speed operation and much higher data storage capacity than typical PC's.

20 Computing systems suitable for user machines and server systems are well known and do not require additional discussion to one of ordinary skill in the art.

Similarly, server software and user software systems are known. In the following discussion, the illustrative embodiment of the present invention uses the World Wide Web, and so the user software is a component referred to as a "web browser." For  
25 example, Netscape NAVIGATOR® by Netscape Communication Corporation is a popular web browser. Another browser is Internet EXPLORER® by Microsoft Corporation.

Data communication is typically achieved by a modem connection over a conventional telephone line, or telephone lines upgraded for DSL service. Other  
30 hardware that can be used include ethernet cards (so-called network interface cards, NIC) which allow connection to an ethernet backbone. Alternative high-speed communication media are becoming available, including cable modem and wireless services, which provide internet access over radio frequency communication channels. These and other communication media are known to those of ordinary skill in the art.

Users 132, 134 further typically include respective printers 142, 144 and other peripheral devices (not shown).

In accordance with the representative embodiment shown in Fig. 1, first server 102 is a web server, providing HTML-based content 112 to users 132, 134. The web server can be any data processing machine or machines running (executing) appropriate system and applications software such as the operating system (OS). Server software running on the first server provides the web content comprising the web pages which constitute a web site. Thus, for example, YAHOO® is a web site comprising numerous web pages that can be accessed by a user. Large web sites typically have multiple server machines to provide adequate system throughput. Thus, each of the servers 102, 104 shown in Fig. 1 may in actuality be one or more physical machines, though logically each is viewed as a single server machine (system).

Flows 103, 105 are data flows between each respective users 132, 134 and first server 102. In accordance with the invention, these data flows are secured. In the context of Internet protocols, secured data communication between a web site and a browser is achieved by the secured sockets layer (SSL) protocol. This is a protocol designed by Netscape Communications Corporation to provide encrypted communications for secured transactions on the Internet. SSL is layered beneath application protocols such as HTTP, SMTP, Telnet, FTP, Gopher, and NNTP and is layered above the connection protocol TCP/IP.

Communications network 122 can be a public switched telephone network (PSTN), a cable modem connection, a locally provided private network (e.g., an intranet), or any of a number of known variations of the foregoing. The communications network may itself comprise many interconnected computer systems and communication links. The communication links may be hardwire links, optical links, satellite or other wireless communications links, wave propagation links, or any other mechanisms for communication of information. While in one embodiment the communications network is the Internet, in other embodiments, the communications network may be any suitable computer network. For example, first server 102 can be accessed over the Internet by users 132, 134. Alternatively, first server 102 can be on the Internet and accessed from within the confines of a business that has a privately maintained network and a gateway to the Internet.

Thus, communications network 122 is not limited to any particular network configuration. Other networking configurations falling within the scope of the



invention as claimed are contemplated. Generally, data communication system 100 depicted in Fig. 1 is merely illustrative of an embodiment incorporating the present invention and is not intended to limit the scope of the invention. One of ordinary skill in the art can readily recognize variations, modifications, and alternatives to the illustrated embodiment.

A secure data communication channel 101 also exists between first server 102 and second server 104. As will become clear below, a secure link is needed to prevent tapping of the channel to avoid fraudulently obtained information from the second server. In the illustrated embodiment of Fig. 1, communications network 122 links first server 102 to second server 104 over data channel 101. This is typically an XML-based (Extensible Markup Language) channel. However, the first and second servers can be linked by alternative secured means. For example, a dedicated land line may be used to provide a secure data link between the first server and the second server. Alternatively, a virtual private network (VPN) could be used to provide a secure channel between servers 102 and 104.

Second server 104 is authorized by a postal authority system 160 to dispense postage. For example, the U.S. Postal Service (USPS) is the organization created by the United States government, which can authorize second server 104 to dispense postage in the same way that today's postage meters are "authorized" to dispense postage. Second server is thus a postage vendor server. Other examples of postal authorities elsewhere in the world include France's La Poste and UK's Royal Mail.

Referring to Figs. 2 and 3, server software 212 running on first server 102, in accordance with the invention, includes functionality to provide a portal through which postage can be distributed from a postage vendor server to users visiting the site being maintained at the first server. For the discussion of the illustrative embodiment which follows, user 132 comprises a WINDOWS®-based OS (e.g., WINDOWS 95) provided by Microsoft Corporation, though it is understood that other OS technologies can be used.

A user gains access to a web site maintained by first server 102, step 302. A "web site" is any computer on the Internet running a World-Wide Web server process. A particular web site is identified by the hostname part of a URL (universal resource locator), which maps to an Internet address. Since first server 102 is simply a computer running many programs, it may host more than one web site. Each "web site" typically has its own World-Wide Web server process 212 and a hostname uniquely associated with the server process. Consequently, the term "web site," "web server," and server

process 212 will be used interchangeably in the following discussion. As a final observation, it is noted in principle that first server 102 may comprise more than one “web site,” each having its associated server process 212. However for the sake of simplicity, the discussion will assume that a single web site is instantiated at the first server.

The server process 212, which effectuates the presence of the “web site,” provides interaction with the user by way of a series of web pages. One of the web pages contains information relating to the purchase of postage. For example, the web site might offer a “communication page” which provides its visitors with a choice of a variety of forms of communication. This might include facsimile transmission capability of locally stored electronic documents, electronic mail (e-mail), conventional postal mail, and so on. In this business model, the “communication page” serves to draw users to the site. This increases the potential for “hits” at this web site, which in turn becomes an incentive for advertisers to post their ads in this site’s web pages.

On the “communication page” are computer graphics representing hypertext links which, when “clicked,” will take the user through a series of web pages that will ultimately allow her to select postage. A first of the series of web pages will typically be a logon screen, where the user is asked to sign onto a user account in order to request postage. It is noted that a logon procedure is not necessary to the practice of the invention.

In step 304, the user selects the desired postage. This step may be as simple as providing a page having a list of graphics (e.g., radio buttons) which identify the postage that can be obtained by the user. Or, it may comprise a series of additional web pages for accessing postage, including web pages to assist in computing the correct postage for a given package and destination, reconciling account balances, and so on. The complexity level will depend on the features that are desired for visitors of the web site, and is not germane to the present invention. In the end, step 304 is intended to produce a selection of postage, which can comprise a single stamp or an order for a variety of postage of different values.

In an alternative business model, a so-called dot-com retailer offering its goods over its web site might provide a web page which facilitates customer returns. The present invention can be used by a dot-com retailer to assist its customers with returns by providing the customer with a quick and easily obtained postage label for the returned item(s). Since the retailer knows the approximate shipping weight of the item, it can

readily compute the required postage. In this case, selection of postage (step 304) simply involves the customer entering some information identifying the goods to be returned, which the dot-com retailer can associate with a postage amount.

In step 306, there is validation of some sort to ensure that sufficient funds exists for payment of the requested postage before the request is processed. In one embodiment, the web site server 102 can maintain user account information in its database 211 for its users. The user account information can be consulted to determine whether to process the request or not. In the dot-com retailer model, the web site account information might comprise information about the goods the consumer. A return authorization code could serve as validation.

In another illustrative embodiment of the invention, the web server 102 can provide off-the-street type purchasing of postage, where individual user accounts do not have to be maintained by the web site. The user would simply provide some sort of valid payment mechanism (e.g., credit card information), afterwhich the web site would continue processing the postage request. This embodiment of the invention has the advantage of simplifying the web site's administration tasks of the web site. It might be appealing to users who want to make an occasional purchase of postage without having to open an account at the web site.

Continuing, server process 212 then sends (step 308) the user's postage request for postage to postage vendor server 104, preferably over a secured communication link. As noted above SSL is a commonly used protocol for secured transactions between a server (e.g., web site) and a user (e.g., web browser). A commonly used protocol for secured communication between server sites is XML. In practice, the web site 102 is likely to receive requests for postage from many users accessing the server concurrently. In some implementations of the invention, it may be desirable for efficiency reasons to bundle the multitude of individual requests into fewer requests that are then communicated to the postage vendor server 104.

In accordance with the illustrated embodiment of the invention, each request for postage sent by web server 102 includes the user's postage request and the user's payment mechanism (e.g., credit card information). The request is then sent to postage vendor server 104 for further processing.

In the dot-com retailer scenario, a customer account database maintained by the retailer typically includes credit card information or the like. When a customer accesses the retailer site to obtain postage for a return, the retailer sends a postage request

to the postage vendor server to obtain the necessary postage. Included in the postage request, is the customer's credit card information.

At step 309, the web site 102 initiates a download of a postage printing software component 202 to the user's system. The download of the postage printing software component preferably, but not necessarily, occurs concurrently with sending postage requests to the postage vendor server for efficiency reasons. The postage printing software component provides a specialized printing capability and printer interface for handling the eventual printing of the postage to produce the indicium. This aspect of the invention is more fully described in U.S. Provisional Patent Application No. 60/216,779, entitled "System And Method Of Printing Labels," filed July 7, 2000. The postage printing software component can be a print DLL (dynamically linked library) software component that is dynamically installed into the OS, a JAVA® script that is downloaded and executed by the browser software, or other printing software implementations or techniques known to those of ordinary skill.

Processing continues in with step 310. For each postage request, the postage vendor server verifies and debits the credit card account of the user requesting postage by an amount according to the requested postage.

In an alternative embodiment of the invention, web site 102 submits payments for requests for postage rather than the users. In this embodiment, the payment mechanism is provided by the web server. For example, the web site may have a corporate credit card which it uses for purchase of postage on behalf of its users, submitting the corporate credit card information with each user request for postage. Payment of postage by the user is arranged between the web site and the user. The web site is responsible for reconciling any account balance issues with its users. This embodiment illustrates a unique aspect of the invention which greatly increases the convenience of purchasing postage over the Internet. For example, a dot-com retailer can provide a postage-guaranteed return policy to its customers as a convenience feature. Whether the payment mechanism is user-provided or web site-provided, the validation step 310 taken by postal vendor server 104 is the same.

If validation is successful, postal vendor server 104 then generates information, ultimately for printing an indicium for each stamp requested in the user postage request (step 312). According to an embodiment of the present invention, the indicium related information generated by the postal vendor server is in accordance with the IBIP specifications. For each indicium, the information for printing the indicium may

include a bitmap of the indicium, a graphical image of the indicium, data representing the indicium, raw data corresponding to the indicium, or any other information which facilitates printing of the indicium. The information for printing the indicium is then communicated from the postal vendor server to web site 102 (step 314).

For example, the postage indicium data (raw data) sda typically contains the following information:

Postage Amount  
Date  
City of Origin  
Postage Meter Number  
Piece Serial Number

This information may be transmitted from the postal vendor server. This is data that has been processed the least. Alternatively, the postal vendor server may transmit fully processed data that is ready for printing. Depending on the printing technology the amount of processing will vary. At one end is a fully processed image, such as a bitmap, that can be sent to printers with minimal intelligence. Moving up the spectrum of sophistication are printers that can understand post-script language. Indeed, the most sophisticated printer might be one that is specifically designed to print postage from the raw data itself. Thus, the “information for printing indicia” is inclusive of the full spectrum of data representations for the postage.

When the web site receives the information for printing the indicium, the information can be enhanced with an image provided by the web site to enhance the postage. Conventional postage stamps oftentimes are printed with a theme; for example, a flower series might consist of stamps in which the background is a print of a state flower. Likewise, the information for printing the indicium received by the web site can be enhanced (step 316) by such images.

Numerous alternatives are possible for supplying the background image. The web site can provide its own pre-designed images and allow the user to select from among many such images. Alternatively, the web site can be configured to allow for user-supplied images (208, Fig. 2). In yet another alternative, third party vendors can be used to provide background images.

In step 318, the information for printing the indicium (optionally enhanced to contain a background image) is then sent to the user at user system 232. The information received by the user is then used to print the indicium. For example, a printer

device 142 coupled to the user system may be used to print the indicium (or indicia) 200. The postage printing software component 202 in the user receives the information and interacts with the user to print the postage, step 320. As mentioned above, the printing aspect of this invention is more fully described in U.S. Provisional Patent Application No. 60/216,779, entitled "System And Method Of Printing Labels," filed July 7, 2000, and U.S. Non-Provisional Patent Application No. 09/708,185, entitled "System and Method of Printing Labels". The postage printing software component 202 automatically initiates an interactive print sequence upon receiving the information, prompting the user through the steps to print out the received postage.

According to an embodiment the indicium may be printed on any suitable medium such as a label, paper, sheet of labels, envelopes, cards, directly on the mail piece/package, or other like media. One or more indicia may be printed at a time. In alternative embodiments of the present invention, the user may store the information for printing the indicia on a storage medium, such as a memory disk, for subsequent printing. This variation of the illustrative embodiment of the invention might be useful in a scenario where the user has many parcels requiring postage, allowing the user to accumulate all the needed postage before printing the postage. In this scenario, the postage printing software component can be written to recognize that a list of postage needs to be printed and prompt the user accordingly.

In yet another alternative embodiment, an off-line print program can be provided on the user system 232 which allows the user to print out the postage at a later time. In this variation of the illustrative embodiment, the user's computer display includes a graphical icon of the off-line print program. The downloaded postage is displayed on the computer display as a series of document icons. In one version, the user employs a commonly used technique known as "drag-and-drop" to initiate off-line print program to print the postage. In this technique, one or more of the document icons representing the previously downloaded postage is (are) selected by the user and dragged over to the icon representing the off-line print program. In another version, the user simply double-clicks the print icon to initiate the off-line print program.

When the off-line print program is initiated, it establishes a communication link to the Internet to obtain the postage printing software component 202. This component may reside on the first server 102, on the postage vendor server 104, or at some other convenient location on the Internet, or on a local network server. Alternatively, the postage printing software component can be hardcoded into to the off-

line print program, or is already installed in the Windows OS as a print DLL. Preferably, the postage printing program is obtained from a location on the Internet and downloaded on a per-use basis. This allows for the postage printing program to be easily maintained and updated to provide new printing features, enhanced user interfaces, and so on. The off-line print program operates as described in U.S. Provisional Patent Application No. 60/216,779, entitled "System And Method Of Printing Labels," filed July 7, 2000, and U.S. Non-Provisional Patent Application No. 09/708,185, entitled "System and Method of Printing Labels".

In a dot-com retailer operation, the initiation of downloading and subsequent printing of postage can be made using a "one-click" technique. The customer desiring to return goods purchased from the retailer simply inputs a number identifying the goods on the retailer's web page. A button is presented to the user, who then simply clicks on it to obtain the needed postage.

As can be gathered from the foregoing discussion, many printing alternatives are available, involving various user interaction paradigms; e.g. automatic printing, drag-and-drop printing, one-click, and so on. It is understood that these and other interaction methods can be easily incorporated into the present invention within the scope of the claims which set forth the invention.

As stated above, the indicium may be printed on a label, paper, or other like medium, or even on the mail piece/package itself. Fig. 4 depicts an exemplary individual pre-printed label 400 on which the indicium may be printed according to an embodiment of the present invention. As shown in Fig. 4, label 400 has serrated edges 402 which not only serve as a security mechanism but also provide an aesthetic look and feel of a conventional U.S. postage stamp. Other security features imprinted on label 400 may include a colored stripe 404, lines of micro-print 406, a label serial number 408, a logo 410, and a watermark 412. These security features may be placed at different locations on label 400. The description of individual pre-printed label 400 depicted in Fig. 4 is intended only as a specific example for purposes of illustrating an embodiment of the present invention. Many other configurations of label 400 are possible having more or fewer features than those depicted in Fig. 4.

The security features shown in Fig. 4 are meant to reduce fraudulent copying or misuse of the label with the indicium printed on it. For example, colored stripe 404 may be in a color, for example, fluorescent pink, which cannot be easily copied by black and white copiers. Micro-print 406 may include the name of the postage vendor

printed in an intricate manner. For example, micro-print 406 may contain the name “Neopost” printed repetitively.

Individual labels may be serialized for increased security and the serial number corresponding to each label may be printed on the label, e.g. serial number 408 depicted in Fig. 4. As part of composing the user postage request (step 308, Fig. 3), the user may be required to enter the serial number of the label on which the indicium is to be printed. The postal vendor system 104 may maintain a list of all valid (available and unused) label serial numbers and serial numbers associated with labels may be invalidated by the postal vendor system after indicia have been printed on the labels. In this manner, misuse or fraud can be detected if a label serial number received from the user refers to an invalidated serial number.

A logo (i.e., a background image) 410 may be an image of a logo of the postage vendor. In alternative embodiments, logo 410 displayed on label 400 may be selected or customized by the user purchasing the postage. Further, logo 410 need not be pre-printed on label 400, but may be downloaded to user system 232 along with the indicium or indicium data and then printed on label 400 (e.g., example, during steps 316 and 318, Fig. 3).

The different features printed on label 400 may be printed in special ink to further increase security. The paper on which label 400 is printed may itself be made of or contain special features to reduce fraudulent use. Further details related to the use of security features are discussed in U.S. Application No. 09/611,375, entitled “Providing Stamps On Secure Paper Using A Communications Network,” filed July 7, 2000.

Fig. 5 depicts a sheet 500 of pre-printed labels according to an embodiment of the present invention. As shown in Fig. 5, sheet 500 comprises ten individual pre-printed labels depicted in Fig. 4. The number of individual labels on a sheet may vary in alternative embodiments of the present invention. Individual sheets may be serialized for increased security and a unique serial number corresponding to each sheet may be printed on the sheet, e.g. sheet serial number 502.

As part of configuring the user postage request, the user may be required to enter the unique serial number of the sheet on which the indicium is to be printed. The postage vendor system 104 may maintain a list of all available and valid sheet serial numbers and the number of unused labels corresponding to the sheets. After all the labels on a particular sheet have been used, the unique sheet serial number corresponding to the particular sheet may be invalidated by the postage vendor system. In this manner, misuse



or fraud can be detected if the sheet serial number received from the user refers to an invalidated sheet serial number. According to an embodiment of the present invention, label serial number 408 printed on each label of a sheet may be the same as sheet serial number 502. In alternative embodiments, the sheets of labels may be serialized using a first set of numbers, and each of the labels on the sheets may themselves be serialized using a second set of numbers. Serializing both the sheets and the labels provides for increased security.

Fig. 6 depicts an individual label 600 with an indicium printed on it according to an embodiment of the present invention. In addition to features of a blank label (described above with respect to Fig. 4), label 600 has an indicium printed on it which may include human readable information and machine readable information. For example, the human readable information of the indicium may include the postage amount or value 602 (e.g. \$0.33), the mail class 604 of the postage (e.g. FIRST CLASS), and number 606 (e.g. 042N5DD00038) corresponding to a PSD resource from the pool of PSD resources on the postage vendor system which was used to generate the information for printing the indicium. Further details related to the use of PSD resources for generating information for printing the indicium are provided below.

The machine readable portion of the indicium may include a two-dimensional code 608, which may be for example a PDF-417 barcode format, a DataMatrix format, or other format. According to an embodiment of the present invention, two-dimensional code 608 is DataMatrix. The particular contents of the two-dimensional code 608 will be discussed below. According to an embodiment of the present invention, the indicium and the positioning of the indicium on label 600 conform generally to specifications described in the IBIP specifications.

Fig. 7 depicts an expanded block diagram of postage vendor system 104 according to an embodiment of the present invention. As shown in Fig. 7, postage vendor system 104 may comprise one or more web servers 702, one or more postal security device module (PSDM) servers 704-1, 704-2 (with associated cryptographic modules 706-1, 706-2), and a database 708 coupled to a local communication network 710 via a plurality of communication links 712. Local communication network 710 provides a mechanism for allowing the various components of postage vendor system 104 to communicate and exchange information with each other. Local communication network 710 may itself be comprised of many interconnected computer systems and communication links. Communication links 712 may be hardwire links, optical links,

satellite or other wireless communications links, wave propagation links, or any other mechanisms for communication of information. The configuration of postage vendor system 104 depicted in Fig. 7 is merely illustrative of an embodiment incorporating the present invention and does not limit the scope of the invention as recited in the claims.

5 One of ordinary skill in the art would recognize other variations, modifications, and alternatives.

Web server 702 may host the postage vendor's web site and store web pages provided by the postage vendor. Web server 702 is responsible for receiving URL requests from user systems 232-1, 232-2 and for forwarding web pages corresponding to the URL requests to the requesting user systems 232-1, 232-2. As previously stated, these web pages allow a user to interact with postage vendor system 104. e.g. to configure a request to purchase postage from postage vendor system 104. When user system 232-1, 232-2 requests communication with postage vendor system 104, web server 702 may be configured to establish a communication link between user system 232-1, 232-2 and postage vendor system 104. For example, web server 702 may establish a secure Internet socket link. e.g. a SSL 2.0 link, between postage vendor system 104 and user system 232-1, 232-2. As noted above, the information communicated between user system 232-1, 232-2 and postage vendor system 104 may be SSL encrypted using various encryption levels, e.g. 40-bit encryption, 128-bit encryption, and the like. Web server 702 may also incorporate a firewall which shields the internal postage vendor system network from communications network 122 and user systems 232-1, 232-2 and other resources coupled to communications network 122. According to an embodiment of the present invention, web server 702 is responsible for receiving requests from user systems 232-1, 232-2 to purchase stamps and for performing load distribution and fail-over processing associated with the requests. Web server 702 may also be configured to control the downloading of printer control programs from postage vendor system 104 to user system 232-1, 232-2.

Each PSDM server 704-1, 704-2, in conjunction with one or more cryptographic modules 706-1, 706-2 coupled to the PSDM server, is responsible for generating the information for printing the indicium in response to requests to buy postage received from one or more user systems 232-1, 232-2. According to an embodiment of the present invention, functions performed by PSDM server 704-1, 704-2 include functions performed by a Postal Security Device (PSD) as described in the IBIP specifications published by the USPS. For example, functions performed by PSDM server 704-1, 704-2 include initialization and creation of PSD resources, digital signature

generation, management of funds related to the postage dispensed by postage vendor system 104, generation of information for printing the indicia, key handling, and other functions. PSDM servers 704-1, 704-2 are designed to operate in a clustered environment to allow for expandability to meet the needs of a rapidly growing user base. According to  
5 an embodiment of the present invention, PSDM server 704-1, 704-2 communicates with web server 702 using a DCOM (Microsoft's Distributed Component Object Model) interface.

Each PSDM server 704-1, 704-2 may comprise one or more cryptographic modules 706-1, 706-2 for performing cryptographic functions and for generating digital  
10 signatures. Various keys for performing security-critical functions such as digital signature generation, hashing, encryption, etc. are stored by cryptographic module 706-1, 706-2. According to an embodiment of the present invention, cryptographic module 706-1, 706-2 is a nCipher nFast/CA module which is validated to FIPS 140-1 Level 3 security.

According to the teachings of the present invention, PSDM server 704-1,  
15 704-2 uses PSD resources to generate indicia and to track monetary amounts related to the postage dispensed by postage vendor system 104. In order to increase the indicia generation throughput, a plurality of shared PSD resources may be used by PSDM servers 704-1, 704-2 to generate the indicia. By using a plurality of PSD resources, multiple PSDM servers 704-1, 704-2 can run concurrently, producing indicia in parallel without  
20 the bottleneck of sharing a single PSD resource.

According to an embodiment of the present invention, each PSD resource comprises a unique PSD identifier (e.g. a 4-byte identifier), a descending register (DR) value (e.g. a 4-byte value), an ascending register (AR) value (e.g. a 5-byte value), and a control code (e.g. a 20-byte value). The PSD identifier uniquely identifies each PSD  
25 resource. The ascending register (AR) value represents the total monetary value of all indicia ever produced by the PSD during its life cycle. The descending register (DR) value indicates the available funds assigned to the PSD resource which may be used to dispense postage. According to an embodiment of the present invention, the monetary values stored by the AR and DR values are measured in 1/10 of 1-cent increments as  
30 specified in the IBIP specifications. The control code is a secure hash of the PSD identifier, the PSD AR value, and the PSD DR value. According to an embodiment of the present invention, the control code is generated using HMAC-with-SHA1 (RFC 2104) using a secret HMAC key stored by cryptographic module 706-1, 706-2.

According to the teachings of the present invention, monetary amounts related to the postage dispensed by postage vendor system 104 are tracked using a global PSD (GPSD) resource and a pool of PSD resources referred to as mini-PSDs (or MPSDs). According to an embodiment of the present invention, eight MPSD resources may be  
5 used by a single cryptographic module 706-1, 706-2 associated with PSDM server 704-1, 704-2 to concurrently generate information for printing indicia. The sum of the AR value and the DR value of the GPSD represents the total amount of postage bought from the postal authority, for example, from the USPS, by the postage vendor provider (e.g. Neopost) of postage vendor system 104. The sum totals of the AR and DR values of the  
10 MPSD resources matches the AR and DR values of the GPSD resource. Information related to the GPSD resource and MPSD resources may be stored in database 708.

According to an embodiment of the present invention, each MPSD resource may be assigned a unique number by the postage vendor. A number assigned to a particular MPSD may be included in the information for printing an indicium generated  
15 by the particular MPSD and printed as part of the indicium. For example, the number “042N50000051” (reference 606 in Fig. 6) uniquely identifies the MPSD resource which was used for generating the information for printing the indicium depicted in Fig. 6. This MPSD serial number is like a meter number and may be used to track the MPSD resource responsible for generating information for printing the indicium. According to an  
20 embodiment of the present invention, the MPSD serial number “042N50000051” may represent a combination of:

- “04” – manufacturer identifier assigned by the postal authority to the postage vendor;
- “2N” – model identifier (details provided below);
- “50000051” – number of MPSDs, which in turn may include for example a global PSD  
25 number “0000”, a machine number “0”, and a PSD number “051.”

Details related to these numbers are provided below. A unique certificate number assigned by a postal authority may also be assigned to each MPSD uniquely identifying the MPSD.

30 Database 708 acts as a repository for storing information related to the postage dispensing process. For example, database 708 may store information related to the PSD resources (both GPSD and MPSDs), information used for generation of digital signatures, and other like information. Database 708 may also store information about users who have purchased postage from postage vendor system 104. Information related

to users who have registered with postage vendor system 104, e.g. user account information, user preferences information, etc. may also be stored by database 708. Database 708 may also store the postal license number assigned to postage vendor system 104 by the postal authority. Other information related to the dispensing of postage may also be stored by database 708. The term "database" as used in this application may refer to a single database or to a plurality of databases coupled to local communication network 710. Further, database 708 may be a relational database, an object-oriented database, a flat file, or any other way of storing information. According to an embodiment, database 708 is coupled to web server 702 and to PSDM server 704-1, 704-2 via an ODBC interface.

Fig. 8 is a simplified flowchart 800 showing processing performed by the various components of postage vendor system 104 upon receiving a request to purchase postage according to an embodiment of the present invention. As shown in Fig. 8 processing is generally initiated when a user using user system 232-1, 232-2 accesses one or more web pages provided by postage vendor system 104 (step 802). Requests to access web pages are generally received by web server 702 which responds by transmitting the requested web pages to requesting user system 232-1, 232-2. As part of the communication, web server 702 may establish a SSL connection with user system 232-1, 232-2. According to an embodiment of the present invention, web server 702 may also download a print control program, such as an ActiveX control or a Netscape plug-in, to user system 232-1, 232-2. The control program may be executed to establish the SSL connection.

Web server 702 may then receive a request from the user to purchase postage (step 804). As previously described with reference to Fig. 3, the request may comprise information such as information identifying the user, a user identifier and a corresponding password if the user is a registered user, credit-card or other like information, the amount and value of the postage to be purchased, the weight of the mail piece/package, and other like information. A user may request the purchase of one or more stamps.

According to an embodiment of the present invention, the user purchase request may be transmitted from user system 232-1, 232-2 to postage vendor system 104 in the form of a data structure in Extensible Markup Language (XML), and may comprise the following:

```
<server.bp_RequestWebStampParams>
```

```

        <LoginID>TestPrint</LoginID>
        <Amount>330</Amount>
        <RateClass>1100</RateClass>
        <FIM>0</FIM>
        <SerialNumber>1966-F8CF</SerialNumber>
        <CCNameOnCard>Joe Customer</CCNameOnCard>
        <CCNumber>0000111122223333</CCNumber>
        <CCExp>0401</CCExp>
    </server.bp_RequestWebStampParams>

```

where:

<LoginID>TestPrint</LoginID> is the user's name (or login name or identifier if the user is a registered user);

<Amount>330</Amount> is the amount of postage to be purchased in 1/1000 of US\$1. For example, 330 = \$0.33;

<RateClass>1100</RateClass> is the value corresponding to a rate class of the postage, for example, "First Class";

<FIM>0</FIM> is a unused legacy field which is set to zero;

<SerialNumber>1966-F8CF</SerialNumber> identifies the medium on which the indicium or indicia are to be printed.

According to an embodiment of the present invention, this field identifies the serial number of the sheet of labels on which the user intends to print the indicia (assuming that the sheet of labels are serialized). This field may also identify the serial number of the label on which the indicium is to be printed. In embodiments of the present invention where both the labels and the sheets are serialized, this field may include one or more label serial numbers and one or more sheet serial numbers:

<CCNameOnCard>Joe Customer</CCNameOnCard> is the user's name as spelled on a credit card which is to be used for consummating the commercial purchase transaction. If the user is a registered user, this field may be blank and postage vendor system 104 may use information provided by the user during registration and stored by postage vendor system 104;

<CCNumber>0000111122223333</CCNumber> is the credit card number which the user intends to use for billing purposes. If the user is a registered user, this field may be blank and postage vendor system 104 may use credit card information provided by the user during registration and stored by postage vendor system 104; and

<CCExp>0401</CCExp> is the credit card expiration date of the credit card which the user intends to use for billing purposes.

For the shown example, the format of the date is month-year (MMYY). If the user is a registered user, this field may be blank and postage vendor system 104 may use the information provided by the user during registration and stored by postage vendor system 104.

It should be apparent that the above described data structure merely illustrates an example of the data and the data format which may be included in the user's request to purchase postage which is communicated from user system 232-1, 232-2 to postage vendor system 104 and is not meant to limit the scope of this invention as recited in the claims. In alternative embodiments of the present invention, more or less information than that shown above may be included in the user request. Further, various different formats may be used for communicating the information to postage vendor system 104.

Web server 702 may then validate the purchase request received from user system 232-1, 232-2 (step 806). As part of the validation step, web server 702 may check the validity of the user, the validity of credit-card information or other like information provided by the user, the validity of information identifying the medium on which the indicia are to be printed, e.g. sheet serial numbers and/or label serial numbers provided by the user, and validity of other information related to the purchase request. Various other validation checks may also be performed according to alternative embodiments of the present invention.

Checking credit card validity may involve checking if the user has provided a valid credit card number, ensuring that the user name on the credit card is valid, ensuring that the credit card has not expired, and getting authorization from the credit card company for the value of the postage and other expenses if any, and other checks. Services provided by companies such as Cybercash and Cybersource may be used to perform the validation. If the user is a registered user with a pre-funded account, web server 702 may determine if the user has sufficient funds in the user's account to pay for the postage to be purchased.

Postage vendor system 104 may perform validation of information identifying the medium on which the indicium is to be printed to ensure against fraudulent use of the indicium. As discussed above, serial numbers may be associated with labels or sheets of labels as security measures to reduce misuse of the postage dispensing system. According to an embodiment of the present invention, postage vendor system 104 maintains a list of all valid or unused serial numbers (sheet serial numbers and/or label serial numbers) in database 708. The serial number of a particular label is invalidated after the label has been used. Likewise, the serial number of a particular sheet of labels is invalidated after all the labels on the particular sheet have been used.

Accordingly, validation fails if the information in the user request contains an invalid (i.e. used) sheet or label serial number.

Web server 702 then checks if any of the validation checks performed in step 806 failed (step 808). If any validation check failed, web server 702 may send a message back to the requesting user system 232-1, 232-2 indicating that the validation was unsuccessful (step 810). The message communicated to user system 232-1, 232-2 may also optionally provide reasons for the failure. The user may then be provided a chance to remedy the reason for the validation failure. For example, if the user is a registered user with a pre-funded account, and web server 702 during the validation process determines that the user does not have sufficient funds in his/her account to pay for the requested postage, the user may be offered the choice of adding funds to the account to enable the transaction to be completed, or the user may be allowed to change the purchase request such that the amended request falls within the limits of available funds. Likewise, if the user has inadvertently provided incorrect information e.g. credit card information, the user may be allowed to correct the information and resend the purchase request to postage vendor system 104.

If it is determined in step 808 that the validation checks performed in step 806 were successful, web server 702 then, based on the purchase request, determines the number of stamps for which information for printing the indicium have to be generated and the tasks for generating the information are allocated to one or more PSDM servers 704-1, 704-2 (step 814). In this manner, web server 702 distributes the indicium related information generation work load among PSDM servers 704-1, 704-2 coupled to local communication network 710. Web server 702 may use different allocation schemes/algorithms to distribute the work among PSDM servers 704-1, 704-2.

According to an embodiment of the present invention, web server 702 maintains a list of all PSDM servers 704-1, 704-2 coupled to local communication network 710. For example, a list of available PSDM servers 704-1, 704-2 may be stored in the Windows NT registry of web server 702. A system administrator may add or remove PSDM servers using a Windows NT registry editor. According to another embodiment, a proxy software (e.g. C++) class may be provided which stores a list of the available PSDM servers 704-1, 704-2. Information related to PSDM servers 704-1, 704-2 may also be stored in database 708. Web server 702 may then use an allocation scheme such as a round-robin scheme to distribute the work. For example, if there are two PSDM servers available, web server 702 will alternate sending indicium printing information



generation requests to the two PSDM servers. According to this embodiment, if the user has requested the purchase of two US\$0.33 stamps, the task of generating information for printing the indicium for the first US\$0.33 stamp will be allocated to the first PSDM server, and the task of generating information for printing an indicium for the second US\$0.33 stamp will be allocated to the second PSDM server. In this manner, web server 702 makes optimal use of available PSDM servers 704-1, 704-2. It should be apparent that various other allocations schemes/algorithms may also be used by web server 702.

As stated above, according to an embodiment of the present invention, web server 702 may communicate with PSDM server 704 using a DCOM interface. For example, a DCOM interface such as “*IPSDStation*,” shown below, may be provided having two functional APIs “*CreateIndicium*” and “*GetStatus*.”

```
interface IPSDStation : IUnknown
{
    HRESULT CreateIndicium //Function API call to create an indicium
    ( [in] unsigned long postage,
      [in,out] struct Indicium* indicium,
      [out] BSTR* strError);
    HRESULT GetStatus //Function API to get status of a PSDM server
    ( [out] struct PSDServerStatus* pStatus);
};
```

where:

“postage” is the amount/value of postage requested;

“indicium” is a pointer to a Indicium structure storing indicium data. The fields of the Indicium structure are described below;

“strError” contains an error message if the creation of indicium data was prevented due to an error; and

“pStatus” points to a PSDServerStatus structure containing information used for monitoring the performance of a PSDM server.

The *PSDServerStatus* structure includes:

```
struct PSDServerStatus{
    long    Uptime;
    long    Throughput;
    long    Load;
    long    Total};
```

where:

“Uptime” indicates how long the PSDM server has been running in days/hours/minutes/seconds;

“Throughput” indicates the number of indicia requests being handled by the PSDM server per second;

“Load” indicates the percentage of load based on the number of virtual PSDs in use; and

“Total” indicates the total number of indicia generated by the PSDM server.

Referring back to Fig. 8, after the task to generate information for printing an indicium for a stamp has been assigned to a PSDM server 704-1, 704-2, the PSDM server then selects a MPSD resource to be used for generating the information for printing the indicium (step 816). According to an embodiment of the present invention, when PSDM server 704-1, 704-2 is initialized, for example during system startup, PSDM server 704-1, 704-2 acquires exclusive rights to one or more MPSD resources stored in database 708 which will be used to service requests for indicia generation. In essence, PSDM server 704-1, 704-2 “checks out” one or more MPSD resources from database 708. In a specific embodiment, each PSDM server 704-1, 704-2 equipped with a cryptographic module 706-1, 706-2 checks out up to eight MPSD resources. After obtaining exclusive rights to the pool of MPSD resources, PSDM server 704-1, 704-2 goes online and waits for requests to generate information for printing indicia. Accordingly, when PSDM server 704-1, 704-2 receives a request to generate information for printing an indicium from web server 702, PSDM server 704-1, 704-2 selects one of the previously checked out MPSD resources for generating the information.

According to an embodiment of the present invention, as part of step 816, if no MPSD resources are available for use when requested from database 708, a new MPSD resource may be automatically generated. The new MPSD resource is assigned a unique identifier, its AR and DR values are set to zero, and a control code value is assigned to it. The requesting PSDM server 704-1, 704-2 is then allowed to check out the new MPSD resource. A signal is communicated to PSDM server 704-1, 704-2 indicating that the MPSD resource is new, and this causes PSDM server 704-1, 704-2 to make a request to add funds (i.e. add funds to the DR value of the MPSD resource) to the MPSD resource to make it usable. The process of funding a MPSD resource is described below.

PSDM server 704-1, 704-2 may then ensure that the selected MPSD resource has sufficient funds to satisfy the postage request (step 818). If the selected MPSD resource does not have sufficient funds to satisfy the postage request, then PSDM server 704-1, 704-2 may perform processing to fund the selected MPSD resource. Further details regarding processing performed by PSDM server 704-1, 704-2 to fund the selected MPSD resource are explained below.

PSDM server 704-1, 704-2 then generates the information for printing the requested indicium using the selected (and sufficiently funded) MPSD (step 820). PSDM

server 704-1, 704-2 adjusts the AR and DR values of the selected MPSD resource corresponding to the value of the requested stamp for which indicium is to be being generated. The AR value of the selected MPSD resource is increased by the amount of the stamp while the DR value of the selected MPSD resource is decreased by the stamp value. The AR and DR values for the MPSDs along with other information related to the MPSDs may be stored in database 708.

The information for printing the indicium generated in step 820 includes a digital signature signed by cryptographic module 706-1, 706-2 coupled to PSDM server 704-1, 704-2. Several different digital signature algorithms may be used to generate the digital signature. These include algorithms identified in the IBIP specifications such the Digital Signature Algorithm (DSA), the Rivest Shamir Adleman (RSA) Algorithm, the Elliptic Curve Digital Signature Algorithm (ECDSA), and others. The digital signature methodology provides data integrity and non-repudiation services. According to an embodiment of the present invention, the digital signature generated by PSDM server 704-1, 704-2 generally complies with the digital signature requirements specified in the IBIP specifications.

According to a specific implementation of the present invention, the digital signature is signed using a DSA private key, for example, a 1024-bit DSA key, stored by cryptographic module 706-1, 706-2. Cryptographic module 706-1, 706-2 may also store additional keys, such as a key used for hashing purposes, and others. According to an embodiment of the present invention, a Hash-based Message Authentication Code (HMAC) key is stored by cryptographic module 706-1, 706-2 and used for hashing. In order to protect the identity of the private and other keys, cryptographic module 706-1, 706-2 may use a master key to encrypt the stored keys. This master key is generally internally stored and cannot be exported in any way outside of cryptographic module 706-1, 706-2. According to an embodiment of the present invention, a Triple Digital Encryption Standard (3DES) master key is used to encrypt the other keys.

The various keys stored by cryptographic module 706-1, 706-2 are generally created when PSDM server 704-1, 704-2 is initialized. The private key, hashing key, and other keys are created, encrypted using the master encryption key and then internally stored by cryptographic module 706-1, 706-2. The public key corresponding to the private key used for signing the information for printing the indicium, for example a public DSA key corresponding to the private DSA key stored by cryptographic module 706-1, 706-2, is then sent to the postal authority to receive a

certificate serial number. The certificate serial number is stored in database 708 and used by PSDM server 704-1, 704-2 in the indicium generation process.

As part of step 820, data related to the process of generating information for printing the indicium may be stored in database 708. For example, financial  
5 information, user information, and other information related to generation of information for printing the indicium may be stored in database 708 by PSDM server 704-1, 704-2 and associated cryptographic module 706-1, 706-2. This information may be downloaded to postal authority system 160 at periodic intervals.

The information for printing the indicium generated in step 820 is then  
10 forwarded by PSDM server 704-1, 704-2 to web server 702 which communicates the information to requesting user system 232-1, 232-2 (step 822). As described above, according to an embodiment of the present invention, PSDM server 704-1, 704-2 may use a DCOM interface (e.g. the IPSDStation interface described above) to forward the generated indicium to web server 702. For example, a call to the "CreateIndicium" API  
15 (described above) returns a pointer to an Indicium structure which is included in the information for printing the information and which contain data representing the indicium. The contents of the Indicium data structure may include:

```
struct Indicium
{
20     byte VersionNo;
        byte AlgorithmID;
        byte CertificateSerialNo[4];
        char ManufacturerID[2];
        char ModelID[2];
25     byte SerialNo[4];
        byte AscendingRegister[5];
        byte Postage[3];
        byte Date[4];
        byte ZIP[4];
30     byte UserID[5];
        byte StampSerialNo[6];
        byte DescendingRegister[4];
        char RateCategory[4];
        byte DigitalSignature[40];
35     };
```

where:

"VersionNo" data field represents the version number assigned by the postal authority, for example, the USPS, to the indicia data set. A 1-byte binary value may be used to represent  
40 this data field;

"AlgorithmID" data field identifies the digital signature algorithm used to create the digital signature in the indicium. A 1-byte binary value may be used to represent this data field;

“*CertificateSerialNo*” data field represents a unique serial number of the PSD certificate issued by the IBIP Certificate Authority (e.g. USPS). A 4-byte binary value may be used to represent this data field;

5 “*ManufacturerID*” data field represents the USPS-assigned identifier for the postage vendor. For example, the manufacturer identifier “04” may be assigned to Neopost. A 2-character ASCII text may be used to represent this data field;

10 “*ModelID*” data field represents the model number assigned to the product model by the postal authority (e.g. the USPS). A 2-character ASCII text may be used to represent this data field e.g. “2N”. According to the IBIP specifications, the first character is this data field is a numeric value (0-9) and the second character is an alphanumeric value (A-Z);

“*SerialNo*” data field represents the serial number of the MPSD used to generate the indicium data. A 4-byte binary value may be used to represent this data field;

15 “*AscendingRegister*” data field represents the total monetary value of all indicia ever generated by the MPSD during its life cycle. A 5-byte binary value may be used to represent this data field;

“*Postage*” data field represents the amount of postage applied for this specific indicium. This data field may be represented using a 3-byte binary value in numeric format. This data field supports the maximum amount of postage due on a single piece of mail in any mail class supported by the mail system;

20 “*Date*” data field represents the date the indicium was printed (from the PSDM server’s clock). This data field may be represented using a 4-byte binary value in the format YYYYMMDD);

25 “*ZIP*” data field represents the ZIP of the user requesting the indicium (also called the originating user). This data field may be represented using a 4-byte binary value in 5-digit numeric format;

“*UserID*” data field identifies the user requesting the indicium. For example, this field may contain the name of the user. If the user is a registered user, this field may contain the user identifier assigned to the user by postage vendor system 104. This data field may be represented using a 5-byte binary value;

30 “*StampSerialNo*” data field is a combination field. The first section (e.g. the first byte) of the field may represent a system software identification number for the PVS software. The second section (e.g. the remaining 5-bytes) of this field may represent the serial number of the label on which the indicium is printed. For example, stamp serial number is Fig. 6 is “13DA-5F45” (reference 408);

35 “*DescendingRegister*” data field represents the postage value remaining on the MPSD. This data field may be represented using a 4-byte binary value;

40 “*RateCategory*” data field represents the postage class for the indicium and rate, including any presort discount level. The rate values for this field are usually provided by the postal authority, for example, the USPS. This data field may be represented using a 4-byte binary value; and

“*DigitalSignature*” data field represents the digital signature.

The size of this data field is a function of the digital signature algorithm used for generating the digital signature. According to an embodiment of the present invention, a

45 40-byte value may be used for this field for a DSA digital signature.

The information for printing the indicium downloaded to requesting user system 232-1, 232-2 may include various types of information representing the indicium (or indicia). According to an embodiment of the present invention, a bitmap or a graphical image representing the indicium may be included in the information for printing the indicium. According to another embodiment of the present invention, indicium data or a data structure comprising information representing the indicium may be included in the information for printing the indicium. According to yet another embodiment of the present invention, a data structure in XML format may be included. The XML format for the data structure may be as follows:

```

10      <Indicium>
          <MeterNumber>042N50000061</MeterNumber>
          <RateClass>1100</RateClass>
          <FIM>0</FIM>
          <LPO>Warrenton, VA</LPO>
15      <Amount>330</Amount>
          <Matrix>AgFA4gEAMDQyTr3w+gIikQEAAEoBAP8uMQEAAAAAH
h0AAACuBwAAAAAesQ0AMTEwMKHVkp9AoLIvuCxwwwowCZT35n5nxxFKfC4VU6s3i22e
QbgPaFQCH53g=</Matrix>
          </Indicium>

```

where:

<MeterNumber>042N50000061</MeterNumber> is the unique serial number of the MPSD used for generating the indicium data structure;

<RateClass>1100</RateClass> is a value corresponding to a rate class, for example "First Class";

<FIM>0</FIM> is a reserved field set to 0,

<LPO>Warrenton, VA</LPO> is an optional origin address;

<Amount>330</Amount> is an amount of postage in 1/1000 of US\$1, for example, 330 = \$0.33; and

<Matrix>AgFA4gEAMDQyTr3w+gIikQEAAEoBAP8uMQEAAAAAHh0AAACuBwAAA  
 AAesQ0AMTEwMKHVkp9AoLIvuCxwwwowCZT35n5nxxFKfC4VU6s3i22eQbgPaFQCH53  
 g=</Matrix> is Base64-encoded binary data representing the indicium data (89 bytes) that is printed as the machine-readable portion of the indicium.

The indicium data encoded in the *Matrix* section may have the format of *structure*

*Indicium* described above.

The information for printing the indicium received by user system from postage vendor system 104 may then be printed using a printer device coupled to user system 232-1, 232-2. The information may also be stored on a computer-readable storage media for subsequent printing of the indicium. In a specific embodiment of the present invention, user system 232-1, 232-2 may convert the indicium data included in the information for printing the indicium to an indicium before printing. As previously

stated, the indicium may be printed on any medium such as a label, sheet of labels, sheet of paper, directly on the mail piece itself, on an envelope, card, etc., but in preferred embodiments the indicia are printed on serialized label stock, possibly incorporating additional security features.

5               As described above, postage vendor system 104 performs and manages funds related to the postage dispensing process via a GPSD resource and MPSD resources. According to an embodiment of the present invention, when postage vendor system 104 is first initialized or booted up, all the AR and DR values of the GPSD resource and the MPSD resources are set to zero. postage vendor system 104 may then  
10 fund the GPSD resource by making a fund purchase from postal authority system 160. For example, postage vendor system 104 may buy US\$100,000.00 worth of postage from the USPS. After this purchase, the DR value of the GPSD is set to US\$100,000.00. The GPSD may then be used to fund the MPSD resources to make them usable to generate information for printing indicia.

15               Although specific embodiments of the invention have been described, various modifications, alterations, alternative constructions, and equivalents are also encompassed within the scope of the invention. The described invention is not restricted to operation within certain specific data processing environments, but is free to operate within a plurality of data processing environments. Additionally, although the present  
20 invention has been described using a particular series of transactions and steps, it should be apparent to those skilled in the art that the scope of the present invention is not limited to the described series of transactions and steps.

Further, while the present invention has been described using a particular combination of hardware and software, it should be recognized that other combinations of  
25 hardware and software are also within the scope of the present invention. The present invention may be implemented only in hardware or only in software or using combinations thereof.

The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense. It will, however, be evident that additions,  
30 subtractions, substitutions, and other modifications may be made without departing from the broader spirit and scope of the invention as set forth in the claims.